



Daily Open Source Infrastructure Report 10 March 2015

Top Stories

- Two California women were convicted March 5 for their roles in a scheme that defrauded union and private health insurance programs of more than \$50 million. – *Torrance Daily Breeze* (See item [17](#))
- The British National Crime Agency arrested an individual in the U.K. March 4 that is believed to be responsible for breaching the U.S. Department of Defense's Enhanced Mobile Satellite Services communication system in June 2014. – *Softpedia* (See item [18](#))
- Two men were arrested for their alleged roles in a spam campaign that made millions of dollars from 2009-2011 by stealing over 1 billion addresses from 8 U.S. email providers, which is considered to be the largest data breach in U.S. history. – *Softpedia* (See item [22](#))
- Thousands remained without Internet and telephone service in the Williamson and Pikeville areas of West Virginia after to high flood waters that took out a main fiber optic line March 5. – *Logan Banner; Associated Press* (See item [23](#))

Fast Jump Menu

PRODUCTION INDUSTRIES

- [Energy](#)
- [Chemical](#)
- [Nuclear Reactors, Materials, and Waste](#)
- [Critical Manufacturing](#)
- [Defense Industrial Base](#)
- [Dams](#)

SUSTENANCE and HEALTH

- [Food and Agriculture](#)
- [Water and Wastewater Systems](#)
- [Healthcare and Public Health](#)

SERVICE INDUSTRIES

- [Financial Services](#)
- [Transportation Systems](#)
- [Information Technology](#)
- [Communications](#)
- [Commercial Facilities](#)

FEDERAL and STATE

- [Government Facilities](#)
 - [Emergency Services](#)
-

Energy Sector

1. *March 9, Pittsburgh Post-Gazette; Associated Press* – (West Virginia) **One killed, two injured in W.Va. mine roof collapse.** A roof collapse at the Cameron Portal of a Murray Energy coal mine in Marshall County, West Virginia, killed one worker and left two others injured March 8. The company issued a statement claiming an accident had occurred at the coal mine and did not provide any additional details.
Source: <http://www.post-gazette.com/local/region/2015/03/08/Roof-Collapse-at-Cameron-Mine-Portal-Possible-Entrapment/stories/201503080217>
2. *March 7, Associated Press* – (North Dakota) **Pipeline leak causes 10,000-gallon spill in McKenzie County.** The North Dakota Department of Health reported March 7 that a Belle Fourche Pipeline Co.-owned pipeline was struck by equipment and ruptured March 6, spilling 10,000 gallons of oil in McKenzie County. Officials stated that the leak was mostly contained to the excavated site and did not pose a threat to public health.
Source: <http://kfgo.com/news/articles/2015/mar/07/pipeline-leak-causes-10000-gallon-spill-in-mckenzie-county/>
3. *March 6, Lexington Herald-Leader* – (Kentucky) **Man who had role in \$3 million Kentucky oil-well scam pleads guilty.** A man pleaded guilty to charges March 6 for his involvement in a scheme that defrauded investors out of \$3 million by misleading them into thinking that oil wells in Kentucky were producing substantial amounts of oil or that production was imminent. Other co-conspirators paid the man to rework some older oil wells and provide guarantees that they would produce a significant amount of oil in order to deceive investors.
Source: http://www.kentucky.com/2015/03/06/3730804_man-who-helped-in-3-million-kentucky.html

[\[Return to top\]](#)

Chemical Industry Sector

4. *March 5, U.S. Department of Labor* – (Illinois) **Blast badly injures 2 at Chicago Heights, Illinois, manufacturing plant.** The Occupational Safety and Health Administration cited Polychem Services Inc., for 6 willful, 1 repeat, and 4 serious safety violations following an inspection of the company's Chicago Heights facility that was initiated after 2 temporary workers were injured in a September 2014 explosion. Proposed penalties total \$110,000.
Source: https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=NEWS_RELEASES&p_id=27528

[\[Return to top\]](#)

Nuclear Reactors, Materials, and Waste Sector

5. *March 6, The News Journal* – (New Jersey) **Radioactive tritium found in ice outside Hope Creek.** An investigation is underway after PSEG Nuclear officials announced March 5 that radioactive tritium was discovered in concentrations of 10 million picocuries per liter below snow and ice hanging from a building at the company's Salem/Hope Creek reactor complex on Artificial Island, New Jersey, a level 500 times higher than federal water quality standards. No groundwater threats have been identified.

Source: <http://www.delawareonline.com/story/news/local/2015/03/06/hope-creek-tritium/24532349/>

[\[Return to top\]](#)

Critical Manufacturing Sector

6. *March 7, NBC News* – (National) **Fiat Chrysler recalls 703,000 vehicles to fix ignition switches.** Fiat Chrysler issued a recall March 6 for 702,578 model year 2008-2010 Dodge Grand Caravan and Chrysler Town and Country minivans and model year 2009-2010 Dodge Journey SUVs for defective ignition switches that could be jarred into the off or accessory position, turning off the engine and disabling the air bags, power steering, and power breaks.

Source: <http://www.nbcnews.com/business/consumer/fiat-chrysler-recalls-703-000-vehicles-fix-ignition-switches-n319121>

7. *March 6, U.S. Consumer Product Safety Commission* – (International) **Rapala recalls StrikeMaster ice augers due to injury hazard.** Normark Corporation, doing business as Rapala USA, issued a recall March 6 for about 3,000 StrikeMaster Lithium Lazer Ice Augers sold at several sporting goods stores in the U.S., from September 2014-January 2015 due to a potential trigger switch failure that could result in the device not powering off, posing an injury hazard.

Source: http://www.cpsc.gov/en/Recalls/2015/Rapala-Recalls-StrikeMaster-Ice-Augers/?utm_source=rss&utm_medium=rss&utm_campaign=Recalls+RSS

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report

[\[Return to top\]](#)

Financial Services Sector

8. *March 7, Associated Press* – (New Jersey; New York) **Wig-wearing bandit robbed bank of more than \$100G.** Authorities arrested and charged a White Plains, New York woman March 5, for allegedly using a paintball gun to rob a Glen Rock Savings

Bank branch in Glen Rock, New Jersey, of more than \$100,000.

Source: <http://www.foxnews.com/us/2015/03/07/wig-wearing-bank-bandit-robbed-bank-more-than-100g/>

For another story, see item [12](#)

[\[Return to top\]](#)

Transportation Systems Sector

9. *March 8, Sioux City Journal* – (Iowa) **JetBlue plane makes emergency landing in Sioux Gateway Airport.** A JetBlue flight from John F Kennedy International Airport in New York to San Francisco International Airport was forced to make an emergency landing at Sioux Gateway Airport in Iowa March 8 due to a sick crew member who was transported to an area hospital. Passengers were placed on another airplane.
Source: http://siouxcityjournal.com/news/local/jetblue-plane-makes-emergency-landing-in-sioux-gateway-airport/article_ff60f650-9ab3-5135-87f4-27b20fa1bf4a.html
10. *March 8, Portland Oregonian* – (Oregon) **Interstate 5 reopens northbound near Delta Park after four-hour closure caused by five-vehicle wreck.** Northbound lanes of Interstate 5 in North Portland reopened after closing for 4 hours following a 5-vehicle accident that injured nine March 7.
Source:
http://www.oregonlive.com/portland/index.ssf/2015/03/interstate_5_reopens_northbound.html
11. *March 7, Fresno Bee* – (California) **Highway 168 in Prather closed due to live electrical wires in roadway.** Highway 168 at Gooseberry Lane in Prather, California, was closed for more than 4 hours March 7 while crews worked to repair damage caused by a vehicle that struck and knocked down a power pole into the roadway.
Source: <http://www.fresnobee.com/2015/03/07/4414587/highway-168-in-prather-closed.html>

[\[Return to top\]](#)

Food and Agriculture Sector

12. *March 9, Krebs on Security* – (International) **Point-of-sale vendor NEXTEP probes breach.** The president of point-of-sale (PoS) vendor NEXTEP Systems confirmed during the week of March 2 reports that the security of systems used at some of its customer locations, which largely includes restaurants, corporate cafeterias, casinos, airports, and other food service venues, may have been compromised. An investigation was initiated due to reports of a pattern of fraud on payment cards used at Zoup restaurants across the U.S. and Canada.
Source: <http://krebsonsecurity.com/2015/03/point-of-sale-vendor-nextep-probes-breach/>

13. *March 7, U.S. Department of Agriculture* – (Texas) **Rio Tex Wholesale Meats recalls ready-to-eat beef products due to possible Listeria contamination.** The Food Safety and Inspection Service announced March 6 that Rio Tex Wholesale Meats issued a recall for about 58,180 pounds of ready-to-eat beef products due to possible Listeria monocytogenes contamination. The recalled products were distributed for hotel, restaurant, and institutional use in Texas.
Source: <http://www.fsis.usda.gov/wps/portal/fsis/topics/recalls-and-public-health-alerts/recall-case-archive/archive/2015/recall-041-2015-release>

[\[Return to top\]](#)

Water and Wastewater Systems Sector

14. *March 9, WYMT 57 Hazard* – (Kentucky) **Water outages continue for some in Harlan Co.** Cumberland Water Works officials worked to restore service for about 150 and 200 city customers that have been without water since outages began around February 20 due to severe weather, flooding that clogged pipes, and in-line breaks in several areas. The water company reported that they hoped to restore all outages during the week of March 9.
Source: <http://www.wkyt.com/wymt/home/headlines/Cumberland-Water-Works--295558131.html>

[\[Return to top\]](#)

Healthcare and Public Health Sector

15. *March 7, Evansville Courier & Press* – (Indiana) **St. Mary's: Patient information compromised in email hack.** St. Mary's Medical Center in Evansville, Indiana, reported March 7 that it notified about 4,400 patients of a January breach after hackers gained access to patients' personal and health information contained in the emails of several hospital employees. The hospital shut down the email accounts and are continuing to investigate the incident.
Source: http://www.courierpress.com/news/local-news/st-marys-patient-information-compromised-in-email-hack_64108117
16. *March 6, San Francisco Chronicle* – (California) **SF General investigates security breach involving patient records.** The University of California, San Francisco announced March 6 that a former doctor who worked at San Francisco General Hospital from 2005 to 2013 illegally removed copies of an unknown number of patient records from the medical center. Public health officials are working with the university to notify patients whose records were stolen.
Source: <http://www.sfgate.com/health/article/SF-General-investigates-security-breach-involving-6119924.php>
17. *March 6, Torrance Daily Breeze* – (California) **San Pedro woman convicted for role in insurance fraud.** Two California women were convicted March 5 for their roles in a scheme that defrauded union and private health insurance programs of more than \$50

million by submitting bills for medically unnecessary procedures to the International Longshore and Warehouse Union and Operating Engineers Union health insurance plans, along with Aetna and Anthem insurance, for beneficiaries who received free or discounted cosmetic surgeries. The women convinced beneficiaries to undergo several medically unnecessary procedures in order to obtain free or discounted cosmetic surgeries.

Source: <http://www.dailybreeze.com/general-news/20150306/san-pedro-woman-convicted-for-role-in-insurance-fraud>

[\[Return to top\]](#)

Government Facilities Sector

18. *March 6, Softpedia* – (International) **Suspected US Department of Defense hacker arrested in UK.** The British National Crime Agency arrested an individual that is believed to be responsible for breaching the U.S. Department of Defense's Enhanced Mobile Satellite Services communication system in June 2014, in the U.K. March 4. The suspect allegedly gained access to contact details and phone numbers of 800 individuals and the International Mobile Station Equipment Identity (IMEI) codes for about 34,400 devices in the 2014 breach.

Source: <http://news.softpedia.com/news/Suspected-US-Department-of-Defense-Hacker-Arrested-in-UK-475120.shtml>

[\[Return to top\]](#)

Emergency Services Sector

19. *March 8, San Jose Mercury News* – (California) **San Jose: Escaped inmate remains at large.** Authorities continued their search March 8 for an inmate who attacked a Santa Clara Sheriff's Office deputy and fled from the Valley Medical Center in San Jose March 6 while he was being treated for an unspecified medical condition. Officials stated that the inmate should be considered dangerous.

Source: http://www.mercurynews.com/ci_27671079/san-jose-escaped-inmate-remains-at-large

20. *March 7, KCBS 2 Los Angeles* – (California) **Rescue equipment worth \$200K stolen from closed San Bernardino Fire Station.** The San Bernardino Fire Department reported March 7 that rescue equipment worth \$200,000 was stolen from a closed fire station in the city after crews noticed the lock was tampered with while they were picking up equipment for training.

Source: <http://losangeles.cbslocal.com/2015/03/07/rescue-equipment-worth-200k-stolen-from-closed-san-bernardino-fire-station/>

[\[Return to top\]](#)

Information Technology Sector

21. *March 9, Securityweek* – (International) **Email spoofing flaw found in Google Admin console.** Security researchers identified a security flaw in the Google Apps Admin console that could have been exploited to gain temporary ownership of any previously unclaimed domain and used to send malicious emails that would not be flagged as suspicious because they came from trusted servers. Google has addressed the vulnerability.

Source: <http://www.securityweek.com/email-spoofing-flaw-found-google-admin-console>

22. *March 7, Softpedia* – (International) **Two arrested in the largest data breach in the US.** Two men were arrested for their roles in what authorities are calling the largest data breach in U.S. history, in which the suspects allegedly made millions of dollars between 2009-2012 by stealing over 1 billion email addresses from 8 U.S. email service providers and used their distribution platforms to send millions of spam emails containing links to Web sites that promoted products through affiliated marketing activities. Authorities continue to search for a third suspect connected to the scheme.

Source: <http://news.softpedia.com/news/Two-Arrested-in-the-Largest-Data-Breach-in-the-US-475156.shtml>

For another story, see item [18](#)

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web site: <http://www.us-cert.gov>

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Web site: <http://www.it-isac.org>

[\[Return to top\]](#)

Communications Sector

23. *March 8, Logan Banner; Associated Press* – (West Virginia) **Major internet outage in Mingo.** Thousands of Suddenlink costumers in the Williamson and Pikeville areas of West Virginia were without Internet and telephone service after high flood waters pulled down over a 300 foot stretch of fiber optic cable that extended across the river near Nolan March 5. Crews worked to determine how to safely reach the cable and reported that there was no estimated date for restoring services.

Source: <http://www.loganbanner.com/news/news/152227690/Major-internet-outage-in-Mingo>

[\[Return to top\]](#)

Commercial Facilities Sector

24. *March 9, WDTN 2 Dayton* – (Ohio) **Adult, 3 children sickened by leak at daycare.** A suspected gas leak at the Grandma’s Child Development daycare facility in Butler Township caused elevated levels of carbon dioxide in the building and the prompted the business to evacuate and close March 9. One adult and 3 children were transported to an area hospital for evaluation.
Source: <http://wdtn.com/2015/03/09/adult-3-children-sickened-by-leak-at-daycare/>
25. *March 9, Marietta Daily Journal* – (Georgia) **Mableton strip mall burns for 2 hours; no injuries reported.** A fire that broke out inside a store of a Mableton strip mall damaged at least 2 other businesses at the shopping center. The roof collapsed above the 3 stores that the blaze engulfed, and several other businesses were damaged by smoke and water.
Source: <http://mdjonline.com/bookmark/26508609-Mableton-strip-mall-burns-for-2-hours-no-injuries-reported>
26. *March 8, WFTV 9 Orlando* – (Florida) **Orange County Walmart back open after suspicious device cleared.** A Walmart store in Orange County, Florida, was evacuated and closed for about 4 hours March 8 while authorities investigated a suspicious package that was later rendered safe. Two different Walmart stores in Florida were evacuated March 6 due to separate phoned bomb threats that were later determined to be unfounded.
Source: <http://www.wftv.com/news/news/local/orange-county-walmart-evacuated-after-suspicious-p/nkQ2p/>
27. *March 8, Glens Falls Post-Star* – (New York) **Route 9 Wal-Mart closed after fire.** Authorities are investigating a fire that broke out inside a Walmart store in Queensbury March 8 and caused an evacuation of the business while crews ventilated the building. Crews worked to assess damage and clear the scene, and the store was scheduled to reopen March 9.
Source: http://poststar.com/news/local/route-wal-mart-closed-after-fire/article_8905ed7e-c5e5-11e4-bd76-ab9c5d7f7c23.html

For another story, see item [12](#)

[\[Return to top\]](#)

Dams Sector

28. *March 9, Associated Press* – (Oregon) **Maintenance, repairs to close dams on Columbia, Snake rivers.** The U.S. Army Corps of Engineers reported that all navigation locks at federal dams on the Columbia and Snake Rivers in Oregon will be closed beginning the week of March 9 for maintenance and repair work. A number of dams are scheduled to resume service March 21 while the remainder will reopen April 4.
Source: <http://www.katu.com/news/local/Maintenance-repairs-to-close-dams-on->

[\[Return to top\]](#)



Department of Homeland Security (DHS)
DHS Daily Open Source Infrastructure Report Contact Information

About the reports - The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for 10 days on the Department of Homeland Security Web site: <http://www.dhs.gov/IPDailyReport>

Contact Information

Content and Suggestions:

Send mail to cikr.productfeedback@hq.dhs.gov or contact the DHS Daily Report Team at (703) 942-8590

Subscribe to the Distribution List:

Visit the [DHS Daily Open Source Infrastructure Report](#) and follow instructions to [Get e-mail updates when this information changes](#).

Removal from Distribution List:

Send mail to support@govdelivery.com.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@hq.dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.